International Association of Oil & Gas Producers

REPORT 677 | JUNE 2024

Lessons in alarm management for well operations

Acknowledgements

This Report was prepared by the Competency and Training Subcommittee (CTSC) of the Wells Expert Committee. IOGP thanks the School of Nuclear Engineering at Purdue University, which conducted the research.

Front cover photography used with permission courtesy of © Ingvar Tjostheim/Shutterstock and © Wlad74/iStockphoto

About

Similarities have been identified between industrial incidents at nuclear power plants and those in well operations, where accidents at site have been attributed to inadequate alarm management design and human error. This Report looks at the lessons learned from the nuclear industry in alarm management practices and provides an insight into how recommended practices can be applied to the management of well operations, including the early detection of well events such as blowouts.

REPORT 677 | JUNE 2024

Lessons in alarm management for well operations

Revision history

VERSION	DATE	AMENDMENTS
1.0	June 2024	First issue

Contents

Acronyms 6

Introduction 7

Background 7

Scope 8

1. Case studies 9

1.1 Three Mile Island 9

1.2 Pryor Trust 10

1.3 Key similarities between TMI and Pryor Trust 11

2. Alarm management objectives 12

2.1 Aiding in initiating prompt operator action 12

2.2 Aiding in determining plant and system status 12

2.3 Aiding in diagnosing and responding to plant transients and events 13

2.4 Facilitating maintenance 13

2.5 Avoiding distracting or overloading users 13

2.6 Exhibiting high reliability and availability 14

2.7 Supporting alarm system performance monitoring 14

2.8 Providing alarm information to other systems and users 14

3. Alarm management challenges and tools 15

3.1 Alarm management challenges 15

3.1.1 Repeating or chattering alarms 15

3.1.2 Multi-setpoint alarms 15

3.1.3 Process variables exceeding normal setpoints 15

3.1.4 Redundant (multi-sensor) alarms 16

3.1.5 System/component state-change alarms 16

3.1.6 Other cause-consequence alarms 16

3.1.7 Maintenance-related alarms 16

3.2 Alarm management methods 16

3.2.1 Preventing or filtering unnecessary alarms 17

3.2.2 Suppressing alarms 17

3.2.3 Highlighting important alarms 17

3.2.4 Changing alarm priorities 17

3.2.5 Adjusting setpoints for process variable alarms 17

3.3 Mitigating alarm overload 17

3.3.1 Time delay filtering and chatter detection 17

3.3.2 Severity-level suppression 17

3.3.3 Redundancy reduction 18
3.3.4 Advanced signal validation 18
3.3.5 Event-based suppression 18
3.3.6 State-based suppression 18
3.3.7 Significance-based suppression 18
3.3.8 Effective alarm prioritization 18
3.3.9 Effective alarm presentation 19

3.4 Alarm management tools 20

3.4.1 Real-time alarm data access 20
3.4.2 Alarm system performance metrics 20
3.4.3 Chattering alarm detection 20
3.4.4 Alarm relationship identification 20

4. Effective alarm management in the nuclear industry 21

5. Considerations for well operations 23

5.1 Suggestions for improvement 24

5.2 State-based alarm implementation 25

5.2.1 Defined operational states 25
5.2.2 State transitions 25
5.2.3 Alarming logic 25
5.2.4 Adaptive thresholds 26
5.2.5 Integration with control systems 26
5.2.6 Operator interface 26

6. Conclusions 27

Appendix A – Lessons from the Three Mile Island accident 28

A.1 Alarm rationalization 28
A.2 Alarm priority 28
A.3 Alarm acknowledgement 28
A.4 Alarm suppression 29
A.5 Operator training 29
A.6 Root cause analysis 29
A.7 Human factors integration 30
A.8 Regular review and optimization 30
A.9 Documentation 30
A.10 Periodic audits 31
A.11 Improved feedback 31

Appendix B – Improvements to the alarm design in nuclear plants 33

Appendix C – Overview of alarm management in nuclear power plants 36

C.1 Alarm management overview 36

C.1.1 Alarm management policies 37

C.1.2 Alarm system requirements and design 37

C.1.3 Alarm selection, definition, and prioritization 37

C.1.4 Alarm configuration management 38

C.1.5 System performance monitoring 38

C.1.6 Periodic assessments 38

C.2 Key alarm functions 39

C.2.1 Alarm detection 39

C.2.2 Alarm generation 39

C.2.3 Alarm processing 40

C.2.4 Alarm presentation 40

C.2.5 Operator aids 41

C.2.6 Alarm response 41

C.2.7 Other aspects of alarm functions 42

C.3 Conventional approaches 43

C.4 Hybrid approaches 44

References 46

Acronyms

DCS	Distributed control system
EPRI	Electric Power Research Institute
ROI	Return on investment
TMI	Three Mile Island
US NRC	US Nuclear Regulatory Commission
VDU	Visual display unit

Introduction

Alarm systems serve a critical role in well operations by continuously monitoring field and equipment conditions and detecting abnormalities that may necessitate operator intervention. They provide visual and auditory alerts to notify operators of situations requiring action, reducing the burden of manually monitoring numerous equipment conditions and process variables. However, while alarms are essential, they present challenges, including alarm overload, the presence of spurious or nuisance alarms, and a lack of clear distinction between alarms and status changes.

Establishing an efficient alarm management system involves transitioning from a notification system with almost random priorities to a genuine operator support tool. This transformation ensures that operators are informed at the right time of the appropriate actions that should be taken, leading to numerous operational advantages and preventing undesirable incidents.

Background

Following the 1979 accident at the Three Mile Island (TMI) nuclear power plant, which resulted in a reactor core meltdown, the nuclear industry and its regulatory bodies have dedicated extensive resources and efforts to revamp and create novel alarm management standards, methodologies, and instruments.

There are similarities between the TMI accident and recent events in well operations (e.g., Pryor Trust), where the cause has been primarily attributed to inadequate alarm management design and human errors and the failure to provide early detection.

Published in 2019, the US Chemical Safety and Hazard Investigation Board investigation report on the Pryor Trust accident noted that: "...most of the alarms would not have been warning of the ongoing well control event... The alarm system would not have been effective in alerting the driller to the imminent blowout."

This conclusion is very similar to that from the Report of the President's Commission on the Accident at Three Mile Island, published in 1979: "Information was not presented in a clear and sufficiently understandable form... Overall, little attention had been paid to the interaction between human beings and machines under the rapidly changing and confusing circumstances of an accident."

The TMI accident served as a pivotal moment, underscoring the critical importance of robust alarm systems in ensuring nuclear plant safety. This endeavour involved a multifaceted approach, by encompassing regulatory reforms, human factors, ergonomics, technological advancements, and profound procedural changes. Regulators have played a pivotal role in imposing stricter alarm management requirements, demanding rigorous adherence to protocols that mitigate human error and reduce the risk of similar incidents. Concurrently, the nuclear industry has witnessed the development of cutting-edge methodologies and tools aimed at streamlining alarm systems, bolstering their effectiveness, and minimizing the likelihood of alarm-related accidents.

The IOGP Wells Expert Committee (WEC) has recognized that important lessons could be learned from the significant improvements in alarm management practices already implemented in the nuclear industry – advancements that can provide essential guidance for enhancing the management of well operations.

Scope

This Report encompasses a comprehensive examination of alarm management systems used in the context of nuclear power plants, with a particular focus on improving their functionality and effectiveness. It addresses various aspects of alarm management, from the definition and prioritization of alarms to their processing and presentation.

It is important to note that this document does not encompass all the requirements necessary for a comprehensive alarm system specification. Instead, it focuses primarily on the most relevant features and capabilities required to achieve specific advancements and to mitigate potential issues that can arise when employing computer-based systems for alarm management systems.

1. Case studies

While the causes and consequences of accidents such as those at the Three Mile Island (TMI) Nuclear Generating Station in Pennsylvania in 1979 and at the Pryor Trust gas well in Oklahoma in 2018 are unique, they are both substantial industrial accidents with significant safety and environmental ramifications. Both accidents were caused mainly by a combination of equipment malfunctions, alarm design-related problems, and operator errors.

Leveraging lessons from the nuclear industry can help address shortcomings and enhance safety measures in well operations.

1.1 Three Mile Island

The TMI accident was a partial meltdown of a nuclear reactor and had a profound impact on the nuclear industry, leading to several improvements in nuclear safety regulations, procedures, and their oversight.

The main causes of the TMI accident were:

- **Equipment errors:** The accident was triggered by a combination of equipment malfunctions. A cooling pump in the reactor's primary coolant loop failed, leading to a loss of coolant and subsequent overheating of the reactor core. Additionally, a relief valve, designed to release excess pressure, failed to close properly, contributing to the loss of coolant.
- **Operator errors:** The control room operators misinterpreted the situation and made errors in responding to the crisis. They believed that the cooling system was functioning properly for several hours, unaware of the severity of the problem. By the time the true extent was understood, a significant portion of the reactor's fuel had already melted.

The TMI accident demonstrated the following issues:

- A surge of alarms was observed
- Numerous alarms were active simultaneously
- Control screens and alarms failed to assist the operators
- There was a lack of a clear process overview for effective diagnosis
- Alarms were being generated at a rate faster than operators could respond
- Critical alarms were not distinctly highlighted or differentiated

System designers failed to account for how the alarms are actually used by the on-site operators. A key lesson was that plant safety should not depend on an operator response to an alarm. Regardless of the design's quality, an alarm system cannot function effectively unless workloads and staffing levels consider all conceivable conditions – from routine operations to disturbances, shutdowns, startups, and emergencies. Operator competence and their requirements must be integral to the new design or modification.

Additionally, users should factor in shift lengths and patterns, human factors, ergonomics, and fatigue considerations, as neglecting these aspects may result in a lack of response precisely when it is most critical.

The lessons learned from the TMI accident can be found in Appendix A. Improvements made since the TMI accident can be found in Appendix B.

1.2 Pryor Trust

The Pryor Trust accident was a blowout and rig fire at a gas well and occurred due to the failure of two crucial safety measures: the primary barrier, involving the hydrostatic pressure created by drilling mud; and the secondary barrier, which relied on human detection of an influx and the activation of the blowout preventer (BOP). These measures were designed to prevent blowouts, but they failed to work as intended.

Several factors contributed to the breakdown of these safety barriers:

- **Equipment errors:** The equipment was set up differently than usual during the tripping operation (e.g., 'tripping wet with the mud bucket aligned to the trip tank'), causing confusion in interpreting the well's data. This confusion led rig workers to overlook signs of gas influx. Moreover, surface pressure was overlooked on two occasions before opening the BOP during operations prior to the blowout, even though there was clearly pressure at the well's surface. This failure to recognize surface pressure played a role in not detecting the gas influx.
- **Alarm design-related problems:** Both the day and night drillers decided to deactivate the entire alarm system, causing them to overlook vital signs of the gas influx and the impending blowout. Additionally, the alarm system to warn personnel about dangerous situations during various operational phases (such as drilling, tripping, circulating, and surface operations) was poorly designed. In the 14 hours before the blowout, the system would have generated numerous non-critical alarms, likely prompting the drillers to disable it to avoid excessive alerts.
- **Operator errors:** Critical flow checks, essential for assessing whether the well was flowing, were neglected prior to the accident. Workers on the drilling rig conducted minimal flow checks, failing to adhere to the company's mandatory checks during well drilling. The drilling contractor did not adequately oversee the compliance with its flow check policy, leading to insufficient monitoring of the implementation rate.

1.3 Key similarities between TMI and Pryor Trust

While the nature of the accidents at TMI and Pryor Trust differs, there are key similarities in terms of equipment errors, alarm design-related problems, and operator errors, as summarized in Table 1.

Table 1: Summary of the key similarities between the TMI and Pryor Trust accidents

Main causes	TMI (1979)	Pryor Trust (2018)
1. Equipment errors	Cooling pump and relief valve failures caused loss of coolant and reactor overheating.	Different equipment setup led to confusion among rig workers, causing an oversight of signs for gas influx.
2. Alarm design-related problems	Flawed alarm system design and misleading instrument readings caused operator misinterpretation.	Entire alarm system deactivated; poor design for different operational phases led to missed gas influx warnings.
3. Operator errors	Operators misinterpreted the situation, believing the cooling system was functional.	Critical flow checks were omitted; drilling contractor failed to ensure compliance with flow check policies, resulting in insufficient monitoring.

2. Alarm management objectives

In nuclear power plants, alarm management systems serve as a critical component for ensuring safety, reliability, operational efficiency, and effective decision-making – essential for complex and highly regulated environments.

This section elaborates on the objectives of these alarm systems.

2.1 Aiding in initiating prompt operator action

The foremost objective of the alarm system is to alert operators promptly to off-normal plant conditions that necessitate their immediate attention and action. These conditions may include equipment malfunctions, deviations from normal operating parameters, and potential safety hazards.

The alarm system should also furnish the operators with clear and concise information regarding the nature of the off-normal condition, as they need to understand the specific issue or parameter that triggered the alarm and then make informed decisions about the appropriate course of action.

The prioritization of alarms is vital. The alarm system should not only convey the existence of an issue but also indicate its priority level. This helps operators differentiate between critical alarms that require immediate attention and those alarms that may be less urgent.

Beyond providing information and prioritization, the alarm system should guide operators in their initial response to the off-normal condition. This guidance may involve suggesting standard operating procedures, emergency protocols, and specific actions to be taken to mitigate or resolve the issue.

2.2 Aiding in determining plant and system status

The alarm system should facilitate the assessment of the operating status of the entire plant, its major systems, and its critical components, by providing operators with information to help them gauge the availability of plant systems and components.

Early warning indicators should assist operators in identifying deteriorating conditions before there is any impact on the plant's operation. In addition, changes in plant and system status should be conveyed to operators in a way that does not overwhelm or distract them from the alarms needing immediate action.

2.3 Aiding in diagnosing and responding to plant transients and events

The alarm system should support the diagnosis of plant transients and events, and aid operators in understanding complex situations. It should facilitate the use of abnormal and emergency operating procedures during critical events, and enable operators to confirm the success of actions taken in response to system alarms.

The system should maintain a historical record of alarms and events, including their occurrence times and their return to normal conditions. Acknowledgement times should also be recorded for reference.

Integration of alarm and event data with plant variable behaviour records should allow a comprehensive analysis for post-event review, performance monitoring, and historical data analysis.

2.4 Facilitating maintenance

The alarm system should alert maintenance personnel to off-normal conditions that require their attention and with a timely response.

Support for collaborative efforts between operations and maintenance personnel is essential for effective issue resolution. The alarm system's features should seamlessly integrate with other maintenance management systems, such as equipment condition monitoring and maintenance work order management. The maintenance and testing of plant systems and equipment linked to the alarm system should be supported, ensuring there is an alignment between plant system testing and alarm system testing.

2.5 Avoiding distracting or overloading users

Avoiding unnecessary distractions is crucial so that operators can focus on critical tasks. As well as being user-friendly, interactions with the alarm system operator interface should be designed to minimize the workload required to navigate the system and respond when necessary.

The alarm system should consolidate alarm information from multiple sources into a coherent interface for efficient assimilation and response. Predictability and comprehensibility of the system interface are essential, and it should not inundate users with excessive information.

2.6 Exhibiting high reliability and availability

Redundancy and fault tolerance features, combined with reliable hardware and software, must guarantee that the alarm system remains functional and data integrity is maintained throughout the plant's lifecycle.

A minimum level of alarm functionality is required during and after accidents and should remain accessible even under accident conditions.

2.7 Supporting alarm system performance monitoring

The alarm system should provide features that enable continuous monitoring of its performance and allow for proactive system maintenance and improvements.

2.8 Providing alarm information to other systems and users

The alarm system should be capable of sharing alarm and event information with other information systems and therefore promote cross-system integration and information exchange.

3. Alarm management challenges and tools

This section identifies fundamental alarm management methods and tools that are either already used or which can be applied in operating nuclear plants, to provide a greater ability in processing and presenting alarms in ways that can improve the usability of the alarm information.

Guidance is also provided on how to avoid worsening the alarm management problem when plants convert to digital systems, due to the tendency for alarms to proliferate with these systems.

3.1 Alarm management challenges

Considerable research has been performed and many alarm processing schemes have been developed in attempts to address the alarm problems in nuclear plants. Some comprehensive reviews of alarm processing systems and related research can be found in the reports by the US Nuclear Regulatory Commission (US NRC – NUREG/CR-6684) and the UK Health and Safety Executive (HSE CRR-166 – Volume 3, Section 6).

The following are the various types of alarm management challenges that can arise, and it is essential that these are understood and addressed effectively.

3.1.1 Repeating or chattering alarms

Description: These alarms occur when a plant variable hovers around the alarm setpoint and causes repeated alarm activations.

Scenario: A temperature gauge fluctuating near a critical threshold may trigger repeated alarms, which potentially leads to operator confusion and fatigue.

3.1.2 Multi-setpoint alarms

Description: Multiple alarm setpoints for a single variable, each indicating different levels of severity, which may lead to multiple alarms for the same variable.

Scenario: A pressure sensor may have multiple alarm thresholds that result in alarms triggered at various pressure levels, each requiring a distinct response, which may cause confusion or conditioning to ignore the alarm.

3.1.3 Process variables exceeding normal setpoints

Description: Plant transients or mode changes can cause process variables briefly to exceed their normal alarm setpoints, which can lead to momentary alarms.

Scenario: During a reactor startup, a temperature parameter may temporarily exceed its usual alarm threshold before stabilizing within the acceptable range.

3.1.4 Redundant (multi-sensor) alarms

Description: Multiple alarms may be generated due to a single plant condition or event, stemming from the presence of redundant sensors on a single variable, multiple instrumentation channels, or multiple parallel mechanical or fluid systems.

Scenario: In a power generation facility, redundant temperature sensors may trigger alarms independently, even though they monitor the same aspect of the system.

3.1.5 System/component state-change alarms

Description: When a system or major component is either shut down or shifts into a new operating mode, lower-level alarms can occur as a normal consequence of the state change.

Scenario: Transitioning a turbine from operation to standby mode may trigger alarms related to pressure or temperature changes associated with the shift.

3.1.6 Other cause-consequence alarms

Description: Logical relationships within a system or between systems, such as automatic actuations or interlocks, can generate alarms as a direct consequence of a previous alarm condition.

Scenario: In a manufacturing plant, the activation of an emergency shutdown system may lead to a cascade of alarms throughout various interconnected systems.

3.1.7 Maintenance-related alarms

Description: These alarms signal conditions requiring maintenance but may not necessitate immediate operator action. They can contribute to operator alarm overload.

Scenario: An alarm indicating a worn-out bearing in a rotating machinery component may not require immediate operator intervention, but it should serve as a notification for scheduled maintenance.

3.2 Alarm management methods

Addressing diverse alarm challenges effectively is crucial for enhancing the overall efficiency, safety, and operator experience in industrial settings.

Alarm management methods encompass a spectrum of approaches, ranging from relatively straightforward processes, such as the selective suppression of alarms based on the current state of the plant, to more advanced methods employing artificial intelligence, rule-based systems, or state-based models, to contextualize alarms.

Some designs focus primarily on prioritization and presentation techniques to help operators manage an abundance of alarms during plant system upsets.

3.2.1 Preventing or filtering unnecessary alarms

By utilizing reduction logic, alarms deemed unnecessary can be prevented from appearing and remain hidden from the operator.

3.2.2 Suppressing alarms

Some alarms can be suppressed, leading to a condensed set off alarms being presented to the operator. However, the suppressed alarms are preserved and can be accessed by the operator if required.

3.2.3 Highlighting important alarms

Critical alarms, unaffected by the reduction logic, can be highlighted, while less critical ones are muted. This approach maintains all alarm information but provides operators with a means of distinguishing between the two categories.

3.2.4 Changing alarm priorities

The priority of affected alarms can be modified, often referred to as 'dynamic prioritization', to emphasize their importance during specific situations.

3.2.5 Adjusting setpoints for process variable alarms

By implementing 'dynamic setpoints', the setpoints for alarms related to process variables can be altered as conditions evolve.

3.3 Mitigating alarm overload

The following strategies serve as valuable tools for mitigating alarm overload, streamlining operator response, and ensuring that crucial alarms receive the attention they deserve in complex industrial environments.

3.3.1 Time delay filtering and chatter detection

Time delay filtering involves the utilization of low-pass filtering or the introduction of time delays (during actuation and clearing) to prevent alarms from repeatedly triggering when a variable fluctuates around a setpoint. This technique also incorporates contact 'debounce'.

Chatter detection and lockout involves the monitoring of the rate of alarm occurrences and the blocking of alarms that exceed a predefined repeat rate.

3.3.2 Severity-level suppression

To prioritize the more critical alarms, lower severity alarms (e.g., LEVEL LOW) may be suppressed when higher severity alarms (e.g., LEVEL LOW-LOW) occur.

3.3.3 Redundancy reduction

Combining alarms from multiple sensors or channels into a single alarm, to prevent multiple individual alarms, helps streamline the operator's response.

3.3.4 Advanced signal validation

Employing techniques that generate a single alarm from a validated signal derived from multiple channels enhances alarm accuracy.

3.3.5 Event-based suppression

Consequential alarms caused by major equipment events, such as pump trips, can be prevented by introducing logic that temporarily blocks related alarms. Similarly, suppressing alarms during system startups or actuations will help avoid unnecessary alerts.

3.3.6 State-based suppression

Logic or 'cutouts' can be implemented to prevent alarms when there is a change in the operating mode of the equipment, such as during planned shutdowns or standby modes. This includes the employment of plant mode-based logic to prevent or suppress alarms during non-power operation modes, such as cold shutdowns.

3.3.7 Significance-based suppression

Operators can focus on the most critical issues when alarms are prioritized on a plant-wide basis and low-priority alarms are suppressed during situations where a high volume of alarms occur.

3.3.8 Effective alarm prioritization

Effective alarm prioritization ensures that operators can respond swiftly to critical alarms and contributes to plant safety and operational efficiency.

Methods used to prioritize alarms have a significant effect on the operator's ability to deal with large amounts of alarm information. These include the following.

3.3.8.1 Priority levels

The alarms are categorized, with the highest-priority alarms demanding immediate attention due to their criticality or risk to the plant. These alarms are presented prominently for operators to address first, followed by the lower-priority alarms.

3.3.8.2 Presentation methods

Fixed-position displays (e.g., annunciator tiles) use techniques such as colour or special flash rates to distinguish the high-priority alarms. Message lists often arrange alarms by priority, ensuring that the most critical alarms are readily visible without scrolling off the screen when numerous lower-priority alarms occur.

3.3.8.3 Global basis

Alarm priorities are typically assigned on a plant-wide basis, requiring decisions on relative priority compared to all other alarms. While some alarms have straightforward priorities, many depend on contextual factors, such as concurrent conditions, system state, plant mode, and dependencies.

3.3.8.4 Suppression and prioritization

Priority serves as a basis for alarm suppression. In the event of a plant upset, a display can show only the high-priority alarms while suppressing lower-priority ones (but accessible upon request). Alarm reduction techniques often involve reassigning suppressed alarms to a low-priority, ensuring that unusual or critical alarms receive operator attention.

3.3.8.5 Closely linked

Alarm prioritization and suppression are closely linked, and any alarm reduction strategy should align with the existing or planned prioritization schemes. Clarity is essential to prevent operator confusion regarding which alarms require immediate focus.

3.3.9 Effective alarm presentation

When implementing alarm reduction strategies in industrial settings, the method of presenting alarms must be considered carefully, as some reduction techniques may be suitable for specific alarm presentations, whereas others may not. Some of the key points to bear in mind are as follows.

3.3.9.1 Severity-based alarm suppression

This is one common reduction technique, where alarms for an analogue variable are suppressed when a more severe alarm occurs (e.g., suppressing a 'LEVEL LOW' alarm when a 'LEVEL LOW-LOW' alarm occurs). This works well for alarm message lists, reducing the operator's message load while preserving essential information.

3.3.9.2 Display type

The choice of alarm presentation method matters. For instance, in conventional light boxes with fixed alarm legends, suppressing a LO level alarm due to a separate LO-LO alarm can be potentially misleading. Operators rely on these fixed tiles as indicator lights, and the absence of the LO alarm might cause confusion. Light boxes often arrange alarms hierarchically, with severity increasing from top to bottom.

3.3.9.3 Alternative displays

To address the issue with fixed alarm legends, alternative display methods can be employed. Computer-generated light box displays can use variable messages on simulated tiles instead. These messages indicate the current severity level of the alarm. While this approach requires operator training, it eliminates the ambiguity associated with fixed tiles.

3.4 Alarm management tools

Several tools exist to provide valuable assistance in managing alarms effectively, enhancing system performance, and uncovering insights from alarm data analysis. They offer the following functionalities.

3.4.1 Real-time alarm data access

Some cost-effective tools provide interfaces compatible with major distributed control systems (DCSs). These interfaces enable separate processing, analysis, and the display of alarm data. For instance, alarm data can be formatted in a standard way, facilitating viewing and analysis through common tools such as spreadsheets.

3.4.2 Alarm system performance metrics

Certain tools continuously monitor the real-time flow of alarm data and gauge the system performance using predefined metrics that encompass aspects such as incoming alarm rates, the duration that alarms remain active (standing time), and the alarm counts sorted by point/ID. They serve as benchmarks and enable the evaluation of performance variations following any enhancements.

3.4.3 Chattering alarm detection

These tools can identify alarms that repeatedly switch on and off rapidly and are commonly known as chattering alarms.

3.4.4 Alarm relationship identification

These tools can pinpoint any associations between alarms. For instance, they can recognize patterns where specific alarms consistently follow others, suggesting a cause-and-effect connection with the initial alarm.

4. Effective alarm management in the nuclear industry

The following recommended practices are used by the nuclear power industry for effective alarm management. These practices are crucial for maintaining operational safety and preventing alarm overload that can overwhelm operators.

While these practices have proven effective in the nuclear industry to manage alarms, reduce operator stress and workload, and enhance overall operational safety. These practices are not currently recommended by IOGP for use in well operations. They are provided here for informational purposes.

- **Prioritize alarms:** Assign priority levels to alarms based on their significance and the required operator response. Ensure that high-priority alarms are easily distinguishable from lower-priority ones, allowing operators to focus on critical issues first.
- **Alarm suppression:** Implement alarm suppression techniques to reduce the number of alarms presented to operators during specific plant conditions or events. This should be done thoughtfully so that important information is not lost.
- **Use of logic:** Apply logical processing to alarms to eliminate or reduce the display of irrelevant or redundant alarms. Logical rules can help determine when alarms should be suppressed or highlighted, depending on the plant's operating state.
- **Operator training:** Provide comprehensive training to operators regarding the alarm system, its logic, and any alarm reduction techniques in use. Operators should understand why alarms are processed in specific ways and how they should respond.
- **Continuous improvement:** Establish a programme for continuous improvement of the alarm system. Regularly review and upgrade alarms to optimize their effectiveness. Collaborate with system vendors to ensure new digital systems align with the plant's alarm management strategy.
- **Simulation testing:** Utilize plant simulators to identify alarm groups that contribute significantly to alarm overload during specific events. Target these groups for improvement and consider introducing operator aids, such as highlighted alarm listings, to assist the operator during critical situations.
- **Avoid complexity:** Avoid implementing overly complex alarm processing schemes that operators may struggle to comprehend. Ensure that changes to alarm logic are well-understood by operators and align with their existing practices.
- **Vendor collaboration:** Actively engage with digital system vendors to define new alarms generated by their systems. Do not assume that vendors understand the plant's specific alarm management needs. Collaborate to ensure that new alarms align with the overall alarm strategy.
- **Procedures and information:** Recognize the importance of procedures and additional information sources in helping operators address underlying issues that trigger alarm activations. These resources can provide valuable guidance and support.
- **Improve existing alarm logic:** Enhance the logic of current alarms. When transitioning to digital platforms, such as DCSs, focus on refining alarm logic. Evaluate both existing and new alarms for their validity, considering changes in definitions and logic to reduce unnecessary alarms during various plant states.

- **Define new alarms with logic:** When introducing new alarms, ensure that appropriate logic is applied from the start to avoid contributing to alarm overload.
- **Simplified methods for reducing alarm overload:** Simplified approaches can significantly improve alarm overload without extensive resource investment. Focus on defining new alarms with alarm reduction in mind and initiate a continuous improvement process. Target specific groups of alarms that are major contributors to the overload and consider implementing operator aids.
- **Identify major contributors:** To reduce the effort required for alarm overload reduction, pinpoint alarms that contribute the most to the problem. Analyse alarm histories for actual plant transients, such as reactor trips, and identify repeating or system state-related alarms. Apply suppression logic to irrelevant alarms.
- **Highlight unusual alarms:** Implement operator aids that highlight unexpected alarms during transients. Utilize plant simulators to identify a core set of expected alarms for major transients. These aids can help operators quickly identify crucial alarms without losing access to all alarm information.
- **Context-aware alarms:** Generate alarms with context-aware logic that considers plant, system, and equipment operating modes. This reduces nuisance alarms associated with mode changes and maintains alarm relevance.
- **Separate status information:** Separate status change events from the alarms requiring operator action. Route status change events to dedicated displays to help operators maintain situational awareness without immediate action.
- **Maintenance notifications:** Differentiate between alarms requiring operator action and those intended for maintenance personnel. Avoid overwhelming operators with alarms meant for maintenance teams.
- **Better support for transients:** Provide alarm presentations and aids that support operators during transients. Offer information to prompt near-term actions, prioritize alarms based on urgency, and allow operators to drill down to detailed information, including cause-consequence relationships and alarm response procedures.
- **Reliability and availability:** Ensure high reliability and availability of alarm systems under both normal and accident conditions. Implement redundancy and fault tolerance to prevent significant loss of alarm functionality due to single failures. Regularly confirm system operation and include features such as a ‘heartbeat’ indicator to indicate system health.

5. Considerations for well operations

The driller's cabinet, also known as the driller's console or control panel, is a critical component and includes an alarm system that is designed to alert operators to potential issues or emergencies during drilling operations. While specific designs can vary between drilling rigs and manufacturers, a typical alarm system in a driller's cabinet includes several main displays and controls that provide visual and auditory alerts for critical conditions, such as high pressure, excessive torque, or equipment malfunctions. These alarms help operators respond promptly to potential issues.

Typical driller's cabinet alarm systems include the following features:

- **Real-time data display:** The display of real-time data related to the drilling operations. Numeric values, charts, and graphs provide a visual representation of the monitored parameters. Operators can quickly assess the current state of the well and drilling equipment. Data should be prioritized and standardized for display.
- **Visual alarms:** Visual indicators, such as flashing lights or colour changes on the displays (red for critical, yellow for cautions, etc.), provide immediate visual alerts for different types of alarms. Visual cues help operators quickly identify the nature of the issue.
- **Auditory alarms:** Audible alarms, often varying in tone or pattern, accompany the visual indicators. Auditory signals are essential, especially in noisy environments, alerting operators even if they are not looking directly at the driller's cabinet.
- **Alarm acknowledgement:** Operators can acknowledge received alarms, indicating that they have seen and understood the alert. Acknowledging alarms is essential to prevent repeated alerts for the same issue.
- **Alarm history:** A log of alarm events and responses is maintained by the alarm system. This historical data is valuable for post-incident analysis and enables operators and engineers to understand the sequence of events that led to an alarm.
- **Alarm settings:** The system allows for the optimization of the alarm settings, such as threshold values for various parameters. Operators can adjust these settings based on specific drilling conditions and wellbore characteristics as specified by the operational procedures.
- **Remote monitoring:** In modern systems, alarms can be remotely monitored by off-site personnel or supervisors. Remote access allows experts to provide guidance and support to on-site operators during critical situations.

Collectively, these features ensure that the alarm system in the driller's cabinet communicates critical information to operators effectively, enabling them to respond promptly and appropriately to ensure the safety of the drilling operation and its personnel.

It is important to note that advancements in technology and automation have led to more sophisticated driller's cabinets with integrated digital displays, real-time data analytics, and remote monitoring capabilities. This may allow for safer and more efficient drilling operations. However, it may also overload the driller with information if not managed properly. The specific features and displays in a driller's cabinet can vary based on the rig's complexity, age, and manufacturer.

5.1 Suggestions for improvement

Alarms in nuclear power plants and well operations share similarities in their fundamental purpose – to alert operators about any abnormal or potentially dangerous conditions. However, there are distinct differences between these two contexts due to the nature of the industries, the complexity of the processes, and the regulatory requirements. Nuclear power plants have a relatively small number of critical alarms compared to the high volume of alarms in well operations, which can sometimes lead to challenges related to alarm prioritization and operator response. In nuclear facilities, alarms are highly prioritized, and alarm management is meticulously designed to avoid overwhelming the operators.

Even though this analysis is neither comprehensive nor universal, and does not apply to all well operations, some of the identified gaps between alarm systems in well operations and alarm systems in nuclear power plants could be addressed by the following suggestions:

- **Alarm prioritization:** The use of alarm prioritization techniques in well operations to be expanded.
- **Training and documentation:** Dedicated alarm training could ensure that operators understand the alarm codes, their meaning, and the appropriate responses.
- **Redundancy:** Ensure sensor redundancy and that critical alarms have redundant notification methods.
- **Emergency shutdown integration:** Critical alarms could be integrated with emergency shutdown systems, allowing immediate cessation of drilling operations in response to severe emergencies.
- **State-based alarms:** Implement a state-based alarm system where alarms are triggered based on the specific state or mode of the system rather than individual sensor thresholds.
- **Separate status information:** Separate status change events from alarms requiring operator action. Route status change events to dedicated displays to help operators maintain situational awareness without immediate action.
- **Maintenance notifications:** Differentiate between alarms requiring an operator action and those intended for maintenance personnel. Avoid overwhelming operators with alarms meant for maintenance teams.
- **Better support for transients:** Provide alarm presentations and aids that support operators during plant transients. Offer information to prompt near-term actions, prioritize alarms based on urgency, and allow operators to drill down to detailed information, including cause-consequence relationships and alarm response procedures.
- **Reliability and availability:** Ensure high reliability, redundancy, and availability of alarm systems under both normal and accident conditions. Implement fault tolerance to prevent significant loss of alarm functionality due to single failures. Regularly confirm system operation and include features such as a 'heartbeat' indicator, to indicate system health.

5.2 State-based alarm implementation

State-based alarms, also known as state-based alarming or state-based control, are a type of alarm system used in nuclear power plants. Unlike traditional alarm systems that trigger at specific threshold values, state-based alarms focus on monitoring the overall state or condition of a system. These alarms are designed to alert operators when the system's behaviour deviates from the expected or predefined states, regardless of the individual parameter thresholds.

State-based alarms are particularly useful in complex systems where the interactions between parameters are intricate and may not be captured adequately by traditional threshold-based alarms. By focusing on system states, these alarms offer a more nuanced and comprehensive approach to monitoring, ensuring that operators are alerted to critical changes in the overall behaviour of the system, and enabling timely responses to prevent accidents or failures.

Implementing state-based alarms in well operations could provide a holistic approach to the monitoring of the drilling process and equipment and enhance the operator's ability to detect complex issues that might not be apparent when considering individual parameters in isolation. By focusing on the overall behaviour of the drilling system, state-based alarms offer a more comprehensive and contextually relevant approach to monitoring, enabling operators to respond promptly to changes in drilling conditions and the potential risks.

The following describes an example of how a state-based alarm system might be implemented in this context.

5.2.1 Defined operational states

Predefined states can be established, based on the overall behaviour of the drilling system. States could include 'Normal Drilling', 'Tripping Out', 'Connection', 'Lost Circulation', and 'Kick Detected'. Each state is defined by a specific combination of drilling parameters, such as pump pressure, mud weight, flow rates, hook load, and rotary speed.

5.2.2 State transitions

The system monitors various parameters simultaneously. When specific parameter combinations fall outside the predefined ranges for a given state, a state transition occurs. For example, a sudden increase in pump pressure followed by reduction in mud level could indicate pack-off/fracture and loss. However, reduction in pump pressure combined with mud level decrease would also indicate loss when drilling into a weak zone.

5.2.3 Alarming logic

State transitions trigger alarms that alert operators to the change in the overall behaviour of the drilling system. These alarms can be visual, auditory, or both, and they indicate not just individual parameter variations but the potential issue indicated by the state change. For instance, a transition to the Kick Detected state could trigger a high-priority alarm, indicating a potential influx of gas or oil into the wellbore.

5.2.4 Adaptive thresholds

Instead of fixed threshold values for individual parameters, adaptive thresholds are set for each state. These thresholds are dynamically adjusted based on the specific drilling conditions and well characteristics. Adaptive thresholds ensure that alarms are triggered based on the context of the current operational state.

5.2.5 Integration with control systems

State-based alarm systems are integrated with control systems and real-time data analysis tools. The system continuously assesses the drilling parameters, identifies state transitions, and triggers alarms. Additionally, these alarms can be integrated with safety shutdown systems, allowing for automatic responses to critical state changes to prevent accidents.

5.2.6 Operator interface

The driller's cabinet displays the current operational state and any state-based alarms. Visual cues, such as colour changes or state icons, indicate the current state, while alarms are presented with clear indications of the state change and potential issue, providing operators with detailed situational awareness.

6. Conclusions

Since the Three Mile Island accident occurred, a lot of important work has been undertaken by the nuclear industry to make operations safer and more effective. Several of the lessons learned and shared in this Report could be considered and applied to enhance safety in well operations.

Alarms in these industries serve the fundamental purpose of alerting operators about abnormal or potentially dangerous conditions. In both environments, the challenges related to alarms, situational awareness, and operator response can arise with safety and financial consequences. Recommended practices for effective alarm management in nuclear power plants have been shown to be crucial for maintaining operational safety and preventing alarm overload that can overwhelm operators. These recommended practices range from alarm prioritization and suppression to standardization, human factors integration, operator training, continuous improvement, simulation testing and training, and simplicity in alarm processing and presentation.

Opportunities for improvements in well operations include the implementation of the alarm prioritization and suppression techniques to address the challenges related to alarm volume and overload, the standardization of alarms, dedicated alarm training to ensure operators comprehend alarm codes, their meaning and the appropriate responses, ensuring sensor redundancy, and the employment of redundant notification methods for critical alarms. Integrating critical alarms with automated emergency shutdown systems would allow immediate termination of operations during severe emergencies.

Simulators have been found effective in the nuclear industry, as well as in aviation, and it is recommended that they be given further consideration to identify any nuisance alarms or alarms contributing significantly to overload during specific events. In addition, separating status change events from alarms requiring operator action and routing them to dedicated displays could potentially help maintain situational awareness without immediate actions being required. Finally, a state-based alarm system, where alarms are triggered based on the specific system state, is recommended.

Implementing these recommendations can contribute to improved alarm management practices in well operations.

Appendix A - Lessons from the Three Mile Island accident

The lessons learned from the TMI accident had a significant impact on alarm management practices in the nuclear industry and led to important improvements. They continue to influence the design and operation of alarm systems, not only in nuclear facilities but also in various other industries, emphasizing the critical role of effective alarm management in ensuring operational safety and preventing accidents.

Some of the key lessons are described in this appendix and are summarized in Table A.1.

A.1 Alarm rationalization

TMI emphasized the need for alarm rationalization so that only essential alarms are activated during emergencies. Having too many alarms can lead to confusion, which can overwhelm operators and lead to delays in their response. Avoid alarm information overload by rationalizing the alarms, and then prioritizing them, based on their importance and relevance to critical situations, and therefore reduce unnecessary alarms.

Relevance to well operations: Well operations involve multiple processes, equipment, and operating parameters that need continuous monitoring. In such complex environments, numerous alarms can be triggered due to various factors. Rationalizing the alarms helps streamline the monitoring process and prevents operators from being overwhelmed by excessive and non-essential notifications.

A.2 Alarm priority

TMI highlighted the importance of prioritizing alarms based on their criticality. Clearly define the alarm priorities. Critical alarms need to be immediately distinguishable from less urgent ones. Clear distinctions between high-priority alarms (indicating serious issues) and low-priority alarms (providing contextual information) help operators focus on the most critical aspects of the situation. Visual and auditory cues can indicate the severity of the alarm, helping operators prioritize their responses.

Relevance to well operations: During well operations, operators need to focus on critical tasks and make rapid decisions. Unnecessary alarms can distract operators and hinder their ability to respond promptly and effectively. By prioritizing alarms, operators can concentrate on the essential notifications, ensuring a more efficient response.

A.3 Alarm acknowledgement

Implement alarm acknowledgement systems to ensure that alarms are not ignored. Alarm acknowledgement confirms that the operator has seen and understood the alarm, preventing the same alarm from recurring without proper attention.

Relevance to well operations: The concept of alarm acknowledgement is highly relevant to well operations as a timely response to critical events is paramount. Ignoring alarms or not acknowledging them can lead to severe consequences, including accidents, equipment failures, and environmental damage. Implementing alarm acknowledgement systems ensures that alarms are not overlooked and promotes swift actions and prevents potential disasters.

A.4 Alarm suppression

Prevent alarm floods (i.e., in a situation where a large number of alarms or notifications are generated simultaneously or in rapid succession within a system or environment) by suppressing non-critical alarms during emergencies. Suppressing unnecessary alarms helps operators focus on the most important issues and prevents distractions during critical situations.

Relevance to well operations: The concept of alarm suppression is highly relevant. Non-critical alarms, especially during emergencies, can cause distractions and divert the operator's attention away from the primary tasks at hand. Operators in well operations need to maintain a high level of focus and alarm suppression ensures that operators are not inundated with a high rate of alarms, allowing them to concentrate on the most critical issues requiring immediate attention. This focused response is essential for mitigating potential risks and ensuring the safety of personnel and equipment.

A.5 Operator training

TMI underscored the importance of comprehensive operator training and specifically the focus on alarm responses during abnormal situations. Training programmes were enhanced to simulate emergency scenarios, allowing operators to practise their responses to alarms effectively and their decision-making skills under pressure.

Relevance to well operations: Comprehensive operator training is highly relevant and ensures that personnel are well-prepared and can respond to alarms and abnormal situations effectively. Training programmes that simulate environments and mirror real-world challenges with various alarm scenarios allow operators to practise their responses and improve their decision-making skills, practise their communication protocols, and develop effective strategies for dealing with diverse emergency situations. Training also ensures that operators are familiar with the alarm system interface, and the alarm prioritization and alarm acknowledgement procedures. This familiarity is vital for operators to interpret alarms accurately and respond appropriately, preventing misunderstandings and minimizing response times during emergencies.

A.6 Root cause analysis

Conduct root cause analyses for alarm-triggering events. Understanding why alarms are triggered helps in refining alarm settings and preventing issues from recurring, and in improving the overall system's reliability.

Relevance to well operations: Root cause analysis is relevant as it helps identify the underlying reasons behind alarm-triggering events. Understanding the root causes of alarm activations helps in identifying potential safety hazards. By addressing the root causes of alarm-triggering events, well operations can significantly enhance the reliability of their systems, which is crucial for timely responses to critical situations, ensuring the safety of personnel, equipment, and the environment.

A.7 Human factors integration

Involve human factors experts in the alarm system design process. Consider human cognitive limitations carefully and design the alarm systems to create intuitive interfaces that align with operators' mental models, making it easier for them to interpret and respond to alarms accurately. Ergonomic and user-friendly interfaces have also become vital when designing control systems and in preventing misunderstandings and errors.

Relevance to well operations: Involving human factors experts ensures that alarm systems are designed with the operators in mind. User-friendly designs enhance operator efficiency and accuracy in interpreting and responding to alarms, which are crucial aspects in the high-pressure and complex operational environments of well operations.

A.8 Regular review and optimization

Regularly review the alarm system performance and optimize the settings based on operational feedback. Systems should evolve and adapt to changing operational needs and the lessons learned from previous incidents.

Relevance to well operations: Regular review and optimization of alarm systems in well operations are essential for adapting to changing conditions, continuous improvement, minimizing false alarms, enhancing operator response, addressing system degradation, data-driven decision-making, risk mitigation, and ensuring compliance with industry standards.

A.9 Documentation

Maintain detailed documentation about the alarm settings, rationalization processes, and operator response procedures. This documentation ensures consistency in alarm management practices and provides a reference for future improvements.

Relevance to well operations: Maintaining this detailed documentation is essential for ensuring consistency, facilitating training, supporting root cause analysis, ensuring regulatory compliance, promoting continuous improvement, preserving institutional knowledge, and enabling efficient troubleshooting in well operations. The documentation serves as a foundation for safe, efficient, and well-informed alarm management practices within the industry.

A.10 Periodic audits

Conduct periodic audits of alarm systems to ensure that they align with industry recommended practices and regulatory standards. Audits can help identify potential issues and the areas for improvement.

Relevance to well operations: Conducting periodic audits of alarm systems in well operations is essential for compliance verification, identification of non-compliance issues, continuous improvement, risk mitigation, operational efficiency, training and awareness, and for benchmarking of performance. These audits contribute significantly to the organization's safety protocols, operational effectiveness, and overall industry standing, ensuring a safer, more efficient, and well-regulated operational environment.

A.11 Improved feedback

The TMI accident highlighted the importance of providing feedback to operators about the consequences of their actions. Clear and immediate feedback helps operators understand the impact of their decisions and adjust their responses accordingly.

Relevance to well operations: Immediate feedback assists operators in identifying and correcting errors promptly. If an action leads to undesirable outcomes, operators can adjust their responses in real-time, preventing the escalation of associated issues. This proactive approach minimizes the impact of mistakes and contributes to a safer operational environment.

Table A.1: Summary of the lessons learned in alarm management and the potential benefits

Lessons learned	Definition	Benefits
Alarm rationalization	The review and optimization of the alarms generated by monitoring and control systems.	Preventing information overload
Alarm priority	The process of assigning importance or urgency levels to different alarms.	Preventing cognitive overload Avoiding distractions
Alarm acknowledgement	The process by which an operator or system user acknowledges receipt and understanding of an alarm or notification generated by a monitoring or control system.	Preventing critical events Ensuring operator accountability Minimizing alarm fatigue Preventing recurrence
Alarm suppression	A functionality that allows operators of automated systems to temporarily suppress or inhibit specific alarms or notifications.	Focusing during events Enhancing situational awareness Minimizing response times Utilizing resources effectively
Operator training	The process of providing education and instruction to equip operators with the knowledge, skills, and competence needed to perform their tasks safely, efficiently, and effectively.	Enhancing operator preparedness Ensuring critical thinking and decision-making Providing familiarity with alarm systems Ensuring continuous improvement

Root cause analysis	A systematic and structured process used to identify the underlying causes of problems or incidents.	Preventing recurring issues Optimizing alarm settings Enhancing system reliability Improving operational efficiency
Human factors integration	A process that aims to optimize the design, operation, and maintenance of alarms by considering human capabilities and limitations. It involves integrating human factors principles into the design and development of alarms to enhance overall performance and safety.	Reducing misunderstandings and errors Enhancing situational awareness
Regular review and optimization	The ongoing process of assessing and refining the alarm system within a control or monitoring environment. The purpose of this practice is to ensure that the alarm system remains effective, relevant, and aligned with the operational needs.	Minimizing false alarms Enhancing operator response
Documentation	The collection of records, information, and documentation related to the design, implementation, and management of an alarm system.	Providing consistency and standardization Ensuring regulatory compliance Enabling efficient troubleshooting
Periodic audits	The scheduled and systematic examination of alarms to assess their compliance with established standards, procedures, regulations, and/or recommended practices.	Identifying non-compliances
Improved feedback	Enhancements made to the information and/or responses provided in response to a particular action, process, or system.	Enhancing learning Promoting proactive responses

Appendix B - Improvements to the alarm design in nuclear plants

Following the TMI accident, significant improvements were made in the alarm, instrumentation, and monitoring systems of nuclear power plants to enhance safety and provide better real-time information for operators.

This included the implementation of:

- Digital control systems for faster and more accurate processing of information
- Advanced sensors that are designed to withstand harsh conditions and provide accurate readings even during emergencies
- Redundant instrumentation to ensure that if one sensor failed, there would be a backup sensor that will provide the essential data
- Safety parameter display systems to provide a centralized and easy-to-read display of critical plant parameters, which will allow operators to quickly assess the plant's status and identify abnormal conditions
- Computerized plant process computers to continuously monitor and analyse plant parameters and detect anomalies and automatically initiate safety measures if needed
- Human-machine interface designs to ensure that operators can quickly and accurately interpret the data presented to them, especially during high-stress situations
- Remote monitoring capabilities to enable external experts to provide assistance and advice during emergencies

A few examples of the changes implemented are shown in Table B.1, and with these improvements, the alarm systems in nuclear power plants became more reliable, informative, and user-friendly. This played a crucial role in improving the situational awareness of operators and their ability to respond effectively to abnormal conditions, thereby enhancing the overall safety of nuclear power plants.

These enhancements, when applied in the context of well operations, could potentially help improve response times and coordination during emergency situations. Clear communication channels and well-designed alarms might aid in alerting crew members promptly, allowing for early detection and for appropriate actions to be taken in the event of a problem.

Table B.1: Alarm design changes in nuclear power plants following TMI

	Implementation	Outcome
Simplification of displays	Complex and cluttered control panels were simplified. Unnecessary information was removed, and essential parameters were prioritized.	Clear, intuitive displays reduced the cognitive load on operators, allowing them to focus on critical information.
Colour-coding	Information was colour-coded to signify different states or levels of importance. For example, normal operating conditions could be displayed in green, while alarms or abnormal conditions were represented in red.	Colour-coding and colour differentiation allowed operators to quickly identify issues.
Alarm prioritization	Alarms were prioritized based on their importance. Critical alarms were presented more prominently and accompanied by distinctive sounds.	Prioritization ensured that operators could distinguish between different alarm levels and respond accordingly.
Procedural displays	Displays were designed to guide operators through procedures. Sequential steps and decision-making processes were displayed clearly.	Display designs helped operators understand the correct sequence of actions during events.
Status indicators	Plant status indicators, such as reactor coolant levels, pressure, and temperature, were prominently displayed. Trends and historical data were often included to provide context.	Status indicators helped operators anticipate potential issues.
User training and familiarization	Operators were trained to use the updated displays and alarms effectively. Training programmes emphasized familiarity with the layout and functionalities of the control panels.	Training ensured that operators could navigate the displays efficiently under normal and emergency conditions.
Standardization	Standardized displays and alarm designs were implemented across different plants.	Standardization ensured consistency in design, allowing operators to adapt more easily when working at different facilities.
Interactive graphical displays	Interactive graphical representations of plant systems were introduced. Operators could click on specific components or areas of the plant on the screen to access detailed information.	Interactive approach facilitated a better understanding of the plant's status.
Redundant alarms	Critical alarms and safety-related indicators were often duplicated or triplicated to ensure redundancy. If one alarm failed or was missed, redundant alarms would continue to alert operators.	Redundancy reduced the risk of overlooking vital information.
Clear and consistent alarm sounds	Alarms were standardized to have clear and distinct sounds. Different types of alarms had unique tones or patterns, allowing operators to identify the nature of the alarm without looking at the control panel.	Consistency in alarm sounds helped reduce confusion during events.
Alarm acknowledgement and confirmation	Operators were required to acknowledge alarms systematically. Alarm confirmation mechanisms were put in place to prevent alarm suppression without operator awareness.	Acknowledgement and confirmation process ensured that each alarm was recognized and dealt with promptly.

	Implementation	Outcome
Human factors analysis	Human factors engineering principles were applied to design alarm systems. Studies were conducted to understand how operators respond to alarms under stress, leading to improvements in the placement, colour, and wording of alarm messages for optimal operator response.	Human factors engineering minimized the operator response.
Multimodal alarms	Alarms were designed to be multimodal, employing both visual and auditory signals. Visual indicators, such as flashing lights or specific colours on the control panel, accompanied audible alarms.	Multimodal alarms ensured that operators received alerts through multiple senses, increasing the likelihood of a timely response.
Dynamic alarm thresholds	Some alarm systems incorporated dynamic alarm thresholds that adjusted based on the plant's operating conditions.	Dynamic alarm thresholds ensured that alarms were triggered at appropriate levels, considering the specific state of the reactor and related systems.
State-based alarms	Different operational states of the nuclear power plant are predefined based on combinations of parameters, such as reactor coolant temperature, pressure, and reactor power level. States could include 'Normal Operation', 'Startup', 'Shutdown', 'Transients' and 'Emergency Shutdown'. Each state is defined by specific parameter ranges and conditions.	State-based alarms enhanced situational awareness, allowing operators to detect abnormal conditions and respond promptly to ensure the safety and stability of the plant.

Appendix C - Overview of alarm management in nuclear power plants

The effective utilization of alarm information hinges on more than just having a capable alarm system; it necessitates a comprehensive alarm management strategy that ensures alarms are accurately defined, appropriately configured, and that modifications to both the alarms and the alarm system are managed effectively as time progresses.

This appendix provides a concise overview of alarm management and the key functions that the alarm system should perform. It also outlines alarm management approaches used in nuclear power plants, with both conventional control rooms and in the more modern designs.

C.1 Alarm management overview

The aspects of alarm management are shown in Figure C.1.

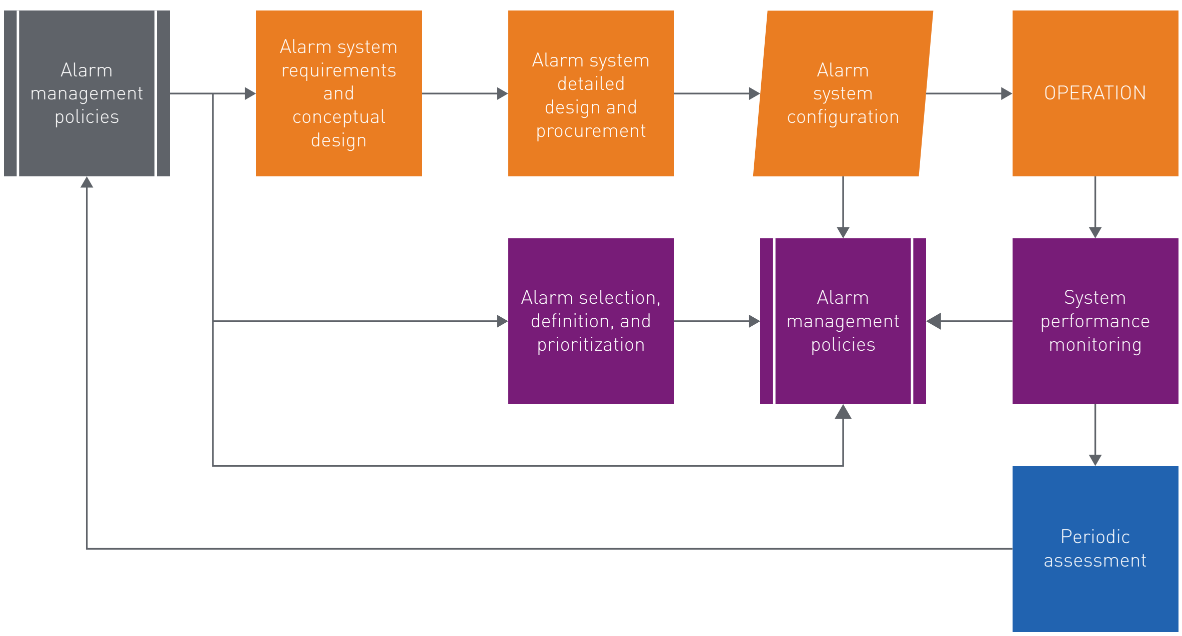

Figure C.1: Alarm management overview and lifecycle

C.1.1 Alarm management policies

This involves the establishing of guidelines for defining alarms and managing configurations, outlining their initial implementation and ongoing management throughout the facility's lifecycle. It is essential to set up appropriate design standards, performance targets, administrative procedures, and alarm management policies. These policies need to align with the facility's 'concept of operations' and 'concept of maintenance'.

Note: The 'concept of operations' pertains to how the plant is run and organized and encompasses aspects such as control room responsibilities, the size and composition of the operating crew, the roles and duties of team members, and the procedures for both normal and emergency operations. The 'concept of maintenance' addresses how maintenance activities are conducted. This includes defining the respective roles of the operating crew and the staff involved in maintenance tasks, establishing the collaboration mechanisms for testing and maintenance support, and outlining the management of maintenance activities and the related information.

C.1.2 Alarm system requirements and design

This involves several key steps, starting with the establishing of the requirements and creating a conceptual design for the alarm system. It then progresses to the detailed design and the procurement of the necessary system components.

C.1.3 Alarm selection, definition, and prioritization

This is a crucial phase in the management of alarms within a facility or system and identifies the alarm conditions (off-normal plant conditions that require operator action) and defines the associated setpoints. This activity should also define the logic and cutouts that may be needed to ensure that the alarm does not occur unnecessarily or as a nuisance (e.g., 'alarm low discharge pressure only if the pump is running').

The process involves several key activities:

1. Selection: This step involves choosing which alarms will be integrated into the alarm system. It requires careful consideration of which events or conditions warrant an alarm, ensuring that alarms are triggered for genuinely important and potentially critical situations.

2. Definition: Once the alarms have been selected, they need to be clearly defined. This means specifying the conditions or events that will trigger each alarm and establishing the precise criteria for when an alarm should activate. Clarity in alarm definitions is essential to prevent confusion among operators and ensure that alarms are triggered appropriately.

3. Prioritization: Alarm prioritization is about ranking the alarms based on their importance or urgency. Some alarms may indicate immediate safety hazards or critical operational issues, while others may be less urgent. Prioritization helps operators focus on the most critical alarms first, ensuring they can respond promptly to high-priority events while addressing lower-priority alarms as time allows.

The effectiveness of an alarm system depends on how well these activities are carried out. Poorly chosen or inadequately defined alarms can lead to operator overload, confusion, and reduced responsiveness to critical conditions. Therefore, a thoughtful approach to alarm selection, definition, and prioritization is vital for maintaining the safety and efficiency of operations within a facility or system.

C.1.4 Alarm configuration management

The next phase includes the configuration of the alarm system, which encompasses the setting of parameters such as alarm thresholds and priorities, deciding how the alarms will be displayed and routed, and configuring the overall display layout.

C.1.5 System performance monitoring

Performance monitoring is crucial, not only to validate the achievement of performance goals initially, but also to maintain ongoing surveillance for issues that may arise during operation. These issues can range from instrumentation problems that cause unnecessary alarms to alterations that have been made to the alarms or the system that have resulted in a degraded performance. Furthermore, regular performance monitoring can unveil opportunities for enhancing the alarms or the alarm system. For example, it may reveal relationships among alarms that could lead to improved logic within the alarm system, resulting in more effective alerts with less redundant information being presented to operators.

C.1.6 Periodic assessments

Regular assessments of performance should be conducted by revisiting the overall alarm management approach. These assessments should aim to evaluate whether existing policies and procedures should be adjusted or refined to enhance long-term performance.

C.2 Key alarm functions

The key functions of an alarm management system are shown in Figure C.2 and are described in the following.

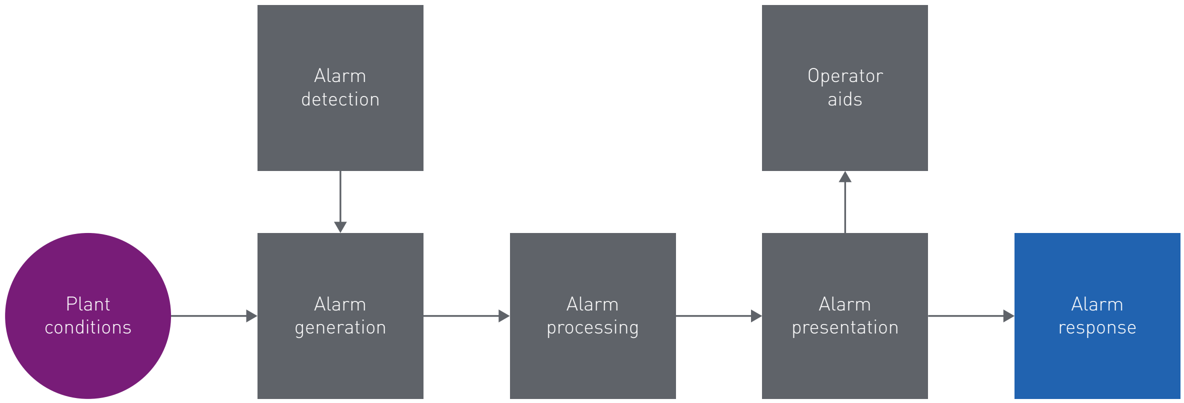

Figure C.2: Key alarm management functions

C.2.1 Alarm detection

Alarm detection occurs when the system identifies a condition or parameter that falls outside the established setpoint boundaries. This detection process may involve complex algorithms and logic to differentiate between normal variations and situations that require operator attention.

C.2.2 Alarm generation

The primary goal of alarm generation is to bring critical conditions to the attention of operators promptly. When an alarm condition is detected, the system generates an alarm signal, which includes essential information, such as the nature of the alarm, the specific parameter that triggered it, and the location or equipment associated with the alarm.

This information is crucial for operators so that they can quickly understand the nature of the issue. To ensure effective communication and decision-making, the alarm system relies on accurate time synchronization among all components. When alarms are generated, the system timestamps them with synchronized time data. This ensures that operators see alarms in the correct chronological order, preventing any confusion or misinterpretation of the sequence of events.

By generating alarms with clear information and correct time references, operators can respond effectively to address the issue. This might involve taking corrective actions, initiating safety protocols, or notifying relevant personnel for further investigation or intervention.

C.2.3 Alarm processing

Once an alarm is generated, processing techniques are employed to assign priorities to the alarms and apply any filtering or suppression actions. Filtering involves the elimination or categorization of the alarms based on predefined conditions, such as suppressing certain alarms, depending on the plant's operational mode.

In a modern alarm system, routing is also a critical function. It involves categorizing the alarms according to the appropriate responders, and then directing them accordingly. Some alarms primarily require maintenance or troubleshooting attention and are addressed by maintenance personnel. These include diagnostic alarms and equipment 'trouble' alarms within the plant. Modern digital systems can identify these alarms and route them to a maintenance workstation, reducing the number of alarms that the operators need to handle.

It is important to note that even if maintenance personnel are the primary responders, operators might still need to be informed about the issue and the need for maintenance. In such cases, the message presented to operators should not contain detailed technical information about the fault, as this level of detail is reserved for the maintenance technician. Instead, the message to operators should convey the significance of the alarm from an operational perspective, guiding them towards any actions they should take. Their response may involve heightened system monitoring, preparing standby equipment for contingency use, or simply understanding that maintenance actions will be required in a specific area.

Finally, alarms should be archived to create a comprehensive alarm history that is accessible to operators, engineers, and maintenance staff, and meets the record-keeping requirements. This archival process should be integrated with other historian functions, such as logging selected process data and equipment operations, as well as recording the sequence of events.

C.2.4 Alarm presentation

The presentation of processed alarm information in a control room can take various forms, each with its own set of advantages and drawbacks. Research has indicated that the most effective approach to alarm presentation is one that offers multiple viewing options, supporting the diverse ways in which alarm information is utilized (as seen in US NRC's NUREG/CR-6691 and EPRI NP-5693P).

Fixed-position alarm tiles are highly effective at alerting operators to abnormal conditions, prompting quick responses when the number of alarms is manageable. They also facilitate rapid situational assessment and can provide an overview of the status of plant systems and equipment. For instance, they can be used to check the availability of systems to aid response planning during plant upsets.

Integrating alarm information into process displays contextualizes the alarms within the broader system, equipment, and process functions. This type of display supports rapid situational assessment at the display level (e.g., for a specific system or function) and aids tasks that rely on this information.

Alarm message lists offer detailed alarm information, including timestamps, setpoint values, current readings, and a more comprehensive description of the alarm condition than what can typically fit on a tile or within a process display. A chronological list of alarm messages assists the operators when examining the progression of a transient event, diagnosing its cause, and identifying any unusual behaviour if the number of alarms is not overwhelming. Alarm reduction techniques can be highly beneficial in managing alarm information overload.

When alarms are presented on multiple types of displays, coordination is crucial to enable operators to seamlessly switch between them and establish connections between the displays. In cases where a DCS is employed, and it controls the light boxes, process displays, and message lists, this integration becomes more manageable. However, when separate annunciators or legacy systems are used, coordinating the alarm displays becomes more challenging.

For more comprehensive guidance on designing alarm displays and information displays in a hybrid control room, the DOE/EPRI hybrid control room guideline (EPRI 1003696) offers valuable information and recommendations.

C.2.5 Operator aids

In addition to the primary alarm displays, which typically consist of fixed-position light boxes, alarm indications on process mimics, and chronological message lists, it is beneficial to create alternative views of alarm information that assist operators in utilizing alarm data for various tasks. These alternative views can encompass different ways of categorizing alarms, such as organizing them by system or by priority, and can also include the outcomes of alarm processing or analysis.

For instance, an operator support tool might offer distinct perspectives on alarms following the application of a suppression scheme. This enables the operator to examine the reduced set off alarms that remain after suppression while also providing access to the alarms that were initially suppressed. Highlighting techniques can be employed to draw attention to alarms that are particularly crucial.

C.2.6 Alarm response

Alarm response is a crucial aspect of maintaining the smooth operation and safety of complex systems, particularly in industrial and process control settings. It involves the provision of well-defined alarm response procedures to guide operators in taking the necessary actions when individual alarms are triggered. In modern digital systems, these procedures can be conveniently displayed electronically on visual display units (VDUs), offering operators a streamlined and efficient means of managing alarms in real-time.

These alarm response procedures often go beyond mere written instructions by integrating live data from the process. This inclusion of real-time data is invaluable, as it allows operators to make informed decisions swiftly when responding to alarms. By presenting relevant process information alongside alarm details, operators can confirm the nature and severity of the alarm condition and take appropriate actions promptly. This real-time data integration not only enhances the response process but also promotes a deeper understanding of the alarm context.

To further expedite the alarm response process, quick access is facilitated through visual cues or hot buttons. These visual or interactive cues serve as immediate pointers to specific response procedures or actions associated with particular alarms. When an alarm is activated, operators can swiftly navigate to the relevant response instructions or actions by simply clicking on the appropriate hot button or following the indicated cue. This minimizes response times and helps ensure that corrective measures are taken promptly to mitigate potential issues or hazards.

In summary, effective alarm response is a critical component for maintaining the safety and efficiency of complex systems. Digital systems have revolutionized this process by electronically displaying comprehensive alarm response procedures, incorporating real-time process data, and providing quick and intuitive access through visual cues and hot buttons. These advancements empower operators to respond swiftly and accurately to alarms, ultimately contributing to the reliability and safety of industrial and process control operations.

C.2.7 Other aspects of alarm functions

Additional aspects of alarm system functions, although not depicted in Figure C.2, play a vital role in the overall effectiveness of alarm systems.

These are essential for comprehensive alarm management, ensuring the system's efficiency, supporting operator and maintenance personnel in their respective tasks, and facilitating effective responses to various alarm scenarios.

C.2.7.1 Alarm administration

This encompasses tasks such as maintaining the alarm configuration database and managing alarms that are temporarily out of service. It also includes the overseeing of operator-defined alarms, those created by operators on a temporary basis to facilitate short-term activities, such as closely monitored equipment.

C.2.7.2 Alarm acknowledgement

This involves the controls and mechanisms for muting auditory alerts (e.g., horns), acknowledging new alarms, and resetting alarms that have returned to a normal state after being triggered.

C.2.7.3 Support for operator tasks

Operators can utilize both the primary alarm information displays and the operator aids mentioned earlier to assist with various tasks. These tasks include assessing the situation, diagnosing plant upsets and events, the planning of responses (e.g., determining the appropriate course of action for restoring critical functions), and obtaining feedback on the outcomes of control actions.

C.2.7.4 Alarm information for maintenance personnel

In digital systems, maintenance personnel have access to workstations equipped with pertinent alarm data and other displays to aid in diagnosing, troubleshooting, and responding to maintenance-related alarms. These alarms provide maintenance staff with distinct messages that offer more precise details about the issue that requires maintenance intervention.

C.3 Conventional approaches

In nuclear power plants with conventional control rooms, as shown in Figure C.3, alarms are presented predominantly through annunciator systems, with supplementary alarm information often relayed via the plant computer. The primary purpose of these alarms is to alert operators promptly to deviations from normal conditions that necessitate their intervention. In most nuclear plants with conventional control rooms, hardwired annunciator systems have traditionally fulfilled this role.

In annunciator systems, an alarm is triggered when a contact either opens or closes. The annunciator electronics detect this change in contact status and provide the operators with both visual and auditory cues to signal the alarm condition.

Visual alerts are typically delivered through conventional light boxes or arrays of alarm tiles with backlit windows. When an alarm condition arises, the corresponding tile starts flashing, providing a visual indication of the issue. Each tile is inscribed with an alarm legend conveying the nature of the alarm condition to the operator. Simultaneously, an audible horn or tone sounds to alert the operator. To cease the flashing indicator and silence the horn, the operator acknowledges the alarm. Subsequently, the tile remains lit steadily until the condition returns to normal. When an alarm condition clears, many annunciator systems reactivate the tile's flashing (often at a different rate) and produce an audible tone, which may differ from the initial alarm tone or horn.

The plant's computer system, or monitoring system, also typically possesses alarm capabilities. These alarms can stem from sensed field contacts, some of which may be shared with the annunciator system, or from process conditions monitored by the plant computer and its data acquisition system. Additionally, alarms can result from calculations performed by the plant computer. In certain plants, the computer may also generate output contact closures that feed into one or more annunciator inputs.

Typically, plant computer alarms have been displayed in the form of message lists, which are shown on one or more visual display units (VDUs) and/or printed on one or more printers. Plant computer alarms may necessitate separate acknowledgement, and they may or may not be accompanied by an audible tone.

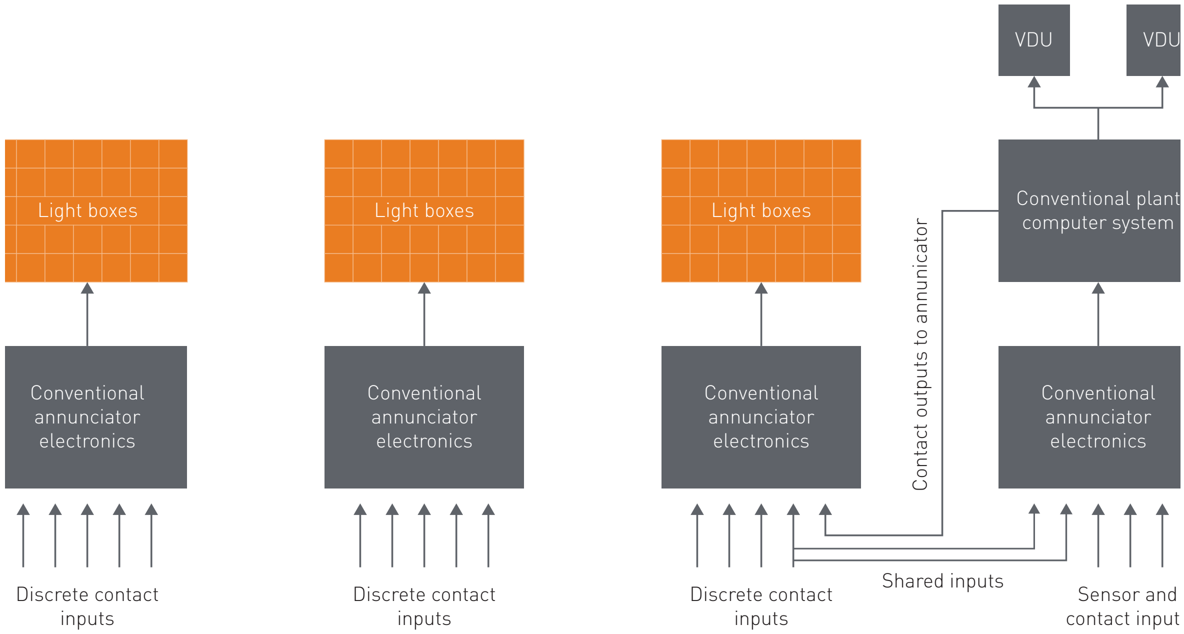

Figure C.3: Example of a conventional control room alarm system

C.4 Hybrid approaches

With advancements in annunciator technology, manufacturers have transitioned from traditional hardwired, single-purpose annunciators to digital microprocessor-based systems, ushering in a host of additional functionalities. These modern annunciator systems offer a range of features, such as:

- **Detailed alarm messages:** Many microprocessor-based annunciators now incorporate VDUs that list detailed alarm messages alongside annunciator windows. This provides operators with more comprehensive information about alarm conditions.
- **Precise timestamps:** Alarms are precisely time-tagged as they are detected, often down to the millisecond. This allows for the creation of a detailed 'sequence of events', presented in chronological lists of messages that can also be printed for reference.
- **Combining multiple alarms:** Several alarm conditions can be combined on a single tile. The VDU then offers a detailed breakdown, indicating which of the various input conditions caused the alarm.
- **Time filtering:** Time delay or time filtering of alarm inputs, including contact 'debounce' filters, can help prevent alarm chattering, where an alarm rapidly toggles between on and off states due to noisy signals.
- **Chatter detection:** Some systems automatically detect and suppress chattering or repeating alarms based on the frequency with which an alarm repeatedly activates and clears.
- **Boolean logic capability:** Certain microprocessor-based systems offer limited Boolean logic capabilities, enabling the creation of more intelligent alarms based on the available input signals.

As plants upgrade their instrumentation and control systems and their control room interfaces, they gain access to a wider array of methods for generating, processing, and presenting alarms. In such hybrid control rooms (i.e., a combination of analogue and digital logic), alarms can be displayed through various means, including traditional light boxes, computer-driven light box replicas shown on VDUs, process monitoring displays such as mimic diagrams, message lists on VDUs, and numerous other display possibilities. The transition to hybrid control rooms means that there may no longer be a single primary alarm system, such as those that existed when annunciators were the primary source of alarm information.

To navigate these evolving options, plants must define their desired control room endpoint and consider interim configurations resulting from staged upgrades. A well-defined strategy should outline how and where alarms will be generated, processed, and displayed at each interim stage and at the final endpoint.

Figure C.4 provides an illustration of various alarm systems that may be part of a hybrid control room design, but it is important to note that the actual configuration will depend on the chosen design concept and specific vendor implementation.

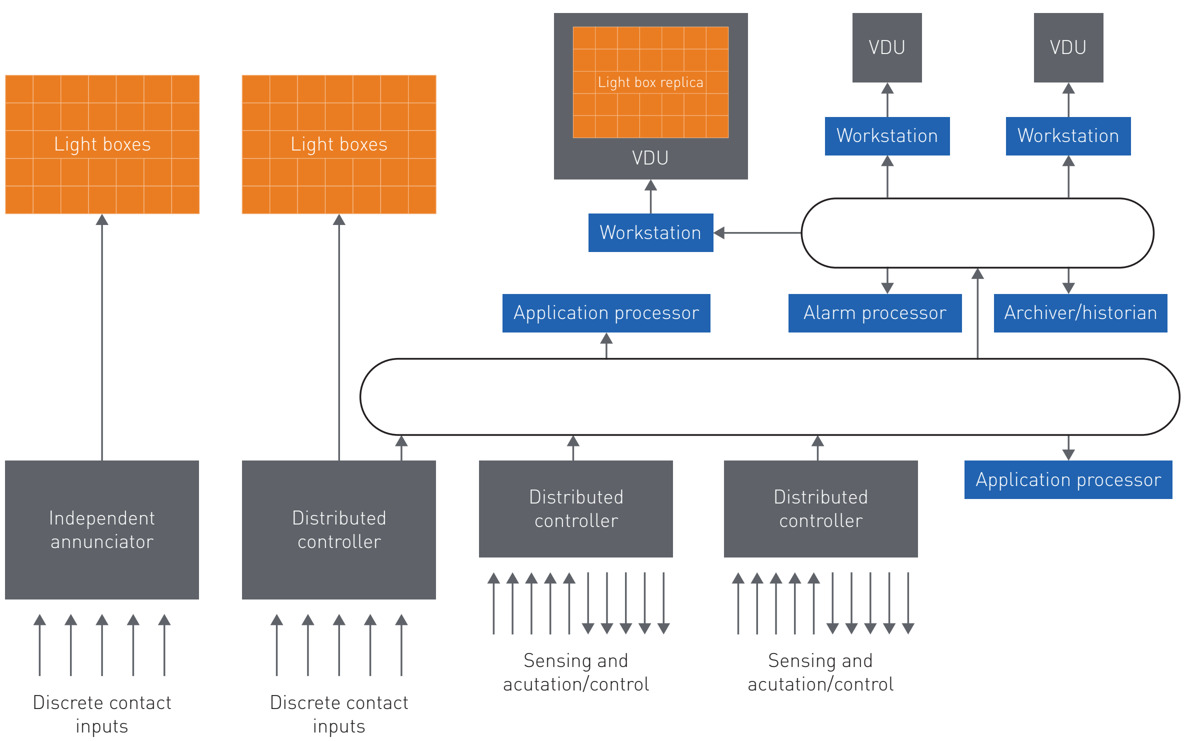

Figure C.4: Example of a hybrid (analogue and digital) control room alarm system

References

Brown WS, O'Hara JM, and Higgins JC. *Advanced Alarm Systems: Revision of Guidance and Its Technical Basis.* NUREG/CR-6684. Washington, DC: US Nuclear Regulatory Commission. 2000.

Electric Power Research Institute. *Alarm Processing Methods: Improving Alarm Management in Nuclear Power Plant Control Rooms.* EPRI, Palo Alto, CA. 1003662. 2003.

Electric Power Research Institute. *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance for Operating Plants and New Builds.* EPRI, Palo Alto, CA. 3002004310. 2015a.

Electric Power Research Institute. *Advanced Control Room Alarm System: Requirements and Implementation Guidance.* EPRI, Palo Alto, CA. 1010076. 2015b.

O'Hara JM et al. *Human Factors Engineering Guidance for the Review of Advanced Alarm Systems*. NUREG/CR-6105. Washington, DC: US Nuclear Regulatory Commission. 1994.

O'Hara JM et al. *The Effects of Alarm Display, Processing, and Availability on Crew Performance*. NUREG/CR-6691. Washington, DC: US Nuclear Regulatory Commission. 2000.

President's Commission on the Accident at Three Mile Island, Washington, DC (USA). "Report of the President's Commission on the Accident at Three Mile Island - The need for change: the legacy of TMI." Washington, D.C. 1979.

US Nuclear Regulatory Commission Office of Nuclear Regulatory Research. *Human-System Interface Design Review Guidelines.* NUREG-0700. Washington, D.C. 1981, 1996, 2002.

US Chemical Safety and Hazard Investigation Board. *Drilling Rig Explosion and Fire at the Macondo Well*. Investigation Report Executive Summary. 2016.

US Chemical Safety and Hazard Investigation Board. *Gas Well Blowout and Fire at Pryor Trust Well 1H-9*. Investigation Report No. 2018-01-I-OK. 2019.

UK Health and Safety Executive (HSE CRR-166 – Volume 3, Section 6)

International Association of Oil & Gas Producers

Similarities have been identified between industrial incidents at nuclear power plants and those in well operations, where accidents at site have been attributed to inadequate alarm management design and human error. This Report looks at the lessons learned from the nuclear industry in alarm management practices and provides an insight into how recommended practices can be applied to the management of well operations, including the early detection of well events such as blowout.

IOGP Headquarters

www.iogp.org

City Tower, 40 Basinghall Street, London EC2V 5DE, United Kingdom
T: +44 20 4570 6879
E: reception@iogp.org

IOGP Americas

T: +1 281 219 9908
E: reception-americas@iogp.org

IOGP Asia Pacific

T: +61 7 2139 9714
E: reception-asiapacific@iogp.org

IOGP Europe

T: +32 2 882 16 53
E. reception-europe@iogp.org

IOGP Middle East & Africa

T: +244 226 434 245
E: reception-mea@iogp.org